National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

Updating SSL to TLS

IAD Mitigations Technical Report

Version 1.0
10 November 2014
MIT-003R-2014

Introduction

Recent media reports confirm that Secure Socket Layer (SSL) 3.0 is obsolete and insecure. This report provides guidance on how to ensure your communications use the more secure Transport Layer Security (TLS) versions while avoiding potential denial of service issues, especially in a federated enterprise setting where it is difficult to coordinate upgrades.

Purpose

This report presents technical instructions for reconfiguring major products using SSL/TLS. It is written for technical managers, cyber defenders, and Information Assurance (IA) analysts who may not be familiar with the specific SSL/TLS implementations in these products.

Background

SSL and TLS are communications protocols that protect end-to-end communications from unauthorized disclosure and modification. SSL and TLS protocols can also authenticate the identity of the end-points in a communication to provide assurance that the participants are who they claim to be. SSL was first implemented in Netscape®[1] products. Version 2.0, introduced nearly a decade ago, was the first version available for public use. It was replaced in 1996 by SSL version 3.0, which was released to address handshake integrity issues that allowed attackers to conduct man-in-the-middle (MITM) attacks. TLS 1.0 was issued as an Internet Engineering Task Force (IETF) standard in 1999, and subsequent versions have been introduced to address security weaknesses, as well as to extend the flexibility of the protocol. TLS 1.2 is the most recent version in use, and provides the most secure and flexible options. SSL and TLS are most commonly implemented in web browsers and servers, but can also be integrated into other products. This report focuses on updating server and browser products. Specific instructions for reconfiguring other security products implementing SSL/TLS may vary, but it is important to update these products as soon as possible.

Details

Recent media reports confirming the obsolescence and insecurity of SSL 3.0 have stirred the industry to take action. Google®[2] researchers published the Padding Oracle On Downgraded Legacy Encryption (POODLE) attack [i] against Cipher Block Chaining (CBC) modes of encryption in SSL 3.0. The Google Advisory shows that there are “no secure SSL 3.0 cipher suites” and that many TLS implementations allow downgrade to SSL 3.0 as part of the support for legacy implementations. Without downgrade protections, and as long as both the server and client allow SSL 3.0, an adversary can induce an automated downgrade to SSL 3.0. Use of SSL 3.0 in environments where MITM attacks are feasible could result in exposure of sensitive data, including protected content on official servers as the result of the recovery of user account information (passwords, cookies, etc.). Other vulnerabilities against SSL v 2.0 also exist, and this version is deprecated in most products. TLS 1.0 and TLS 1.1 are not impacted by the recent attack, but they lack security features that are available in TLS 1.2. Even where MITM attacks

[1] Netscape® is a registered trademark of AOL, Inc.

[2] Google® is a registered trademark of Google, Inc.

are not feasible, server upgrades are required to support browser settings for clients who might be subject to these attacks. There exist dependencies in the order a component should implement mitigations:

1. Reconfigure servers to enable TLS versions 1.0 to the most current version supported.
2. Reconfigure browsers to enable TLS 1.0 or better and disable SSL v 3.0 and earlier SSL versions.
3. Reconfigure servers to disable all SSL versions (2.0 and 3.0).

1. Guidance for Servers:

System owners should focus first on updating servers that only support SSL 3.0. This removes obstacles for updating browsers to disable SSL 3.0. Once browsers are updated, it is possible to disable SSL 3.0 at all servers and move to more secure TLS versions.

Most current servers support SSL 3.0 by default. Organizations hosting sensitive information on servers that allow use of SSL 3.0 should disable SSL 3.0 and enable TLS 1.2, as well as TLS 1.1 and TLS 1.0 as needed for interoperability according to vendor instructions. Instructions to inspect and update the SSL/TLS configuration from major server vendors are indicated in Table 1. If the servers' critical customer base includes a significant number of users on obsolete operating systems with browsers only supporting SSL 3.0, it is reasonable to delay disabling SSL 3.0, but only until those users have enabled at least TLS 1.0, and to implement additional mitigations according to Section 3. Section 2 gives instructions on how to update browsers, even on obsolete operating systems as old as Windows NT.

Table 1: Server Configurations to Disable SSL 3.0

Server	Configuration Notes
Apache®[3]	Run the following commands: SSL Protocol All – SSLv2 –SSLv3 apachet1 configtest sudo service apache2 restart
NginX®[4]	Run the following commands: SSL_protocols TLSv1 TLSv1.1 TLSv1.2; sudo nginx –t sudo service nginx restart
IIS®[5]	See Advisory 2014/3009008 at www.technet.microsoft.com/library/security and follow the directions to disable SSL 3.0 in Windows.
Apple OSX®[6] servers	Update to the latest OSX server version • Mountain Lion: OSX server v 2.2.5 or above • Maverick: OSX server v 3.3.2 or above • Yosemite: OSX server v 4.0 or above

[3] Apache® is a registered trademark of Apache Software Foundation.

[4] NginX® is a registered trademark of NginX Software Inc.

[5] IIS® is a registered trademark of Microsoft Corp.

[6] Apple OSX® is a registered trademark of Apple Inc.

OpenSSL®[7] libraries	See OpenSSL Security advisory [15 Oct 2014] • OpenSSL 1.0.1: upgrade to 1.0.1j • OpenSSL 1.0.0: upgrade to 1.0.0o. • OpenSSL 0.9.8: upgrade to 0.9.8.zc
Other libraries	Use vendor guidance.

Individual servers that implement SSL/TLS in libraries that are not covered by these instructions will require vendor guidance. Scripts to test a web server to see if it supports SSL 3.0 are available through a number of services—use a trusted service or fully test the scripts prior to use in an operational system. Two tests (see Table 2) are required:

a. The first test should determine the versions supported by a server or browser. Any server or browser not configured to use TLS 1.2 should be configured to do so or updated to a version that does. Servers not able to support TLS 1.0 or better should be updated immediately.
b. The second test should confirm that SSL 3.0 is disabled. If it is not possible to disable SSL 3.0, additional mitigations described in Section 3 are required.

Table 2: Tests for SSL

SSL Version Test	Server Response	Recommendation
Display highest version supported	Only SSL 3.0	If possible, immediately reconfigure to support TLS 1.2 (allow TLS 1.1 and TLS 1.0 if necessary for interoperability); If not possible, upgrade immediately to a secure channel library that supports TLS 1.2.
	Highest supported is TLS 1.0	If possible, configure server to support TLS 1.2; If not possible, plan for upgrade.
	Highest supported is TLS 1.1	
	TLS 1.2 is supported	OK
Is SSL 2.0 or 3.0 supported	Connection allowed	If possible, disable SSL 2.0 and 3.0; If not possible, immediately implement downgrade protections and plan for upgrade to a secure channel library that allows SSL 2.0 and 3.0 to be disabled.

[7] OpenSSL® is a registered trademark of Apache Software Foundation.

	Connection refused	OK

2. Guidance for Browsers:

Account information including session cookies and passwords can be exposed if the browser supports SSL 3.0. Many browsers are available that support TLS 1.2, and those that do not should be updated.

For browsers that do not support TLS 1.0 or better (see Table 3), an immediate upgrade is required. More generally, IAD recommends the most recent browsers that support TLS 1.2 (see Table 4) as well as TLS 1.0 and TLS 1.1 (for interoperability). Browsers supporting fallback protection mechanisms are recommended.

Table 3: Obsolete Browsers Unable to Support TLS 1.0 or Better

Browser Version	**Used in**
IE®[8] v3 (no TLS 1.0 support)	Obsolete Windows OS, System 7, Mac OS through v10.4
IE v3 – 6	Obsolete Windows OS, Windows XP (prior to SP3)
Opera®[9] v 3 – 4	Windows, OSX, Android, BlackBerry, Windows Mobile

Most browser vendors have already deprecated SSL 2.0 and are planning updates to deprecate SSL 3.0 and integrate downgrade protections. The Information Assurance Directorate (IAD) recommends installing the most recent browser versions as they become available. Until those updates are available, most current browsers still support SSL 3.0 and require reconfiguration to disable it. Configure these browsers according to the instructions (see Table 4) to block all SSL versions (SSL v2 and SSL v3), use TLS 1.2, and allow TLS 1.1 or 1.0 for interoperability. Include additional mitigations indicated in Section 3 to ensure that downgrade attacks are mitigated.

It should be noted that mission critical servers should be tested (and properly configured) before reconfiguring browsers to disable SSLv3. If mission-critical web servers only support SSL v3, these sites likely will not be viewable in reconfigured browsers.

Table 4: Browsers Supporting TLS 1.2

Browser Version	**Used in**	**To isable SSL versions and enable TLS**

[8] IE® is a registered trademark of Microsoft Corp.

[9] Opera® is a registered trademark of Opera Software ASA.

Chrome™[10] v 30	Various OS	Launch using the command line flag “--ssl-version-min=tls1”
FireFox®[11] v 24 – v 33 Firefox v 34 (when available)	Various OS	For versions 24-33, install the add-on at https://addons.mozilla.org/en-US/firefox/addon/ssl-version-control; or Type **about:config** in the address bar (click ok through any warnings) and search for ‘TLS’. If secrurity.tls.version.min exists set its value to 1. Note: setting security.tls.version.max to 3 enables TLS 1.2. Search for SSL. If ‘security.enable_ssl3’ exists, set its value to false. If ‘security.enable_ssl2’ exists, set its value to false. Note: to enable TLS versions set ‘security.enable_tls to true. Restart the browser and re-run the test[ii].

IE v 11	Windows 7, 8.1; Windows Mobile 8.1	See Advisory 2014/3009008 at www.technet.microsoft.com/library/security
		or
		Select tools->internet options;
		Select the ‘Advanced tab’ and scroll to Security;
		Uncheck the ‘Use SSL 2.0’ and ‘Use SSL 3.0’ boxes;
		Click OK;
		Restart.

Opera v 17 and above	Windows, OSX, Android	Type Opera:config in the address bar and search for ‘SSL’; Uncheck ‘Enable SSL V3’; Restart.

[10] Chrome™ is a trademark of Google.
[11] FireFox® is a registered trademark of Mozilla Foundation.

Safari®[12] v8	iOS 8.5	Update to iOS 8.5 to block CBC modes in SSL v3. Available at http://support.apple.com/kb/ht1222
Safari v8	OSX 10.10	Install security update 2014-005 to block CBC modes in SSL v3. Available at http://support.apple.com/kb/ht1222

For older versions of Windows OS, it might not be possible to implement the recommended version of IE that includes support for TLS 1.2. While it is highly recommended that these older OS versions be updated, we provide instructions (see

Table 5) specific to these systems that will provide access to the most up-to-date version of TLS supported.

Table 5: Browser TLS version support for older operating systems

OS Version	Browser Version	Configuration Notes

NT[iii]	IE 6	Disable SSL 2.0;
		Cannot disable SSL 3.0;
		Enable TLS 1.0;

	Firefox v 2[iv] or above	Disable SSL 2.0;
		Disable SSL 3.0;
		Supports TLS 1.0

	Opera v 10 or above	Disable SSL 3.0; Enable TSL 1.2 and TLS 1.1

XP[v]	IE 8	Disable SSL 2.0;
		Disable SSL 3.0;
		supports TLS 1.0

	Firefox v 12 or above	All versions support TLS 1.0. See Table 4 to disable SSL 2.0

[12] Safari® is a registered trademark of Apple Inc.

		and SSL 3.0
	Chrome	See Table 4
	Opera	See Table 4

Vista®,
Windows 7®,
Windows 8®[13]
	IE 10	Disable SSL 2.0;
		Disable SSL 3.0;
		TLS 1.0 is enabled by default;
		Enable TLS 1.1 and 1.2

iOS v 5-8[vi]	Safari v5-8	Does not support SSL 2.0;
		Cannot disable SSL 3.0;
		Supports TLS 1.2

OSX 10.9[vii]	Safari v7-8	Does not support SSL 2.0;
		Cannot disable SSL 3.0;
		Supports TLS 1.2

3. Additional guidance:

Other applications using SSL should be upgraded to use current TLS versions as well. SMTP, SIP, VOIP, and LDAP products using SSL v3.0 should be updated according to vendor instructions. Products that embed SSL version for management support should also be updated. These applications do not necessarily advertise the use of SSL, and it is up to the vendors to update their security mechanisms. It is always advised to use the most recent versions of security products to take advantage of security updates.

Since upgrading critical servers may take time, it may be necessary to allow some SSL v3 connections to avoid adverse mission impact. In these cases, browsers will need to continue to support SSL v3, and additional mitigations are required for defending against MITM attacks:

a. Configure the browser to block the use of RC4 when using SSL v3.

b. Maintain downgrade protection by disabling additional TLS versions as the risk to using those increases. Consider the risks of using any version less than the most recent (currently TLS 1.2), since newer versions implement mitigations against security weaknesses in previous versions. In addition, some newer browsers enable downgrade protections through the use of a TLS_FALLBACK_SCSV flag that alerts servers that a renegotiation has occurred. Servers that recognize this mechanism will drop a flagged connection if the negotiated version is less than they support. This can be used to prevent attempts to reduce the security for sites that support TLS 1.0 or above.

[13] Vista®, Windows 7®, Windows 8® are registered trademarks of Microsoft Corp.

c. Use application firewalls to block attempts to access non-critical sites supporting only SSL 3.0.

d. Implement further mitigations against MITM attacks. These include ensuring that connections use DNS-SEC to determine IP addresses, and implementing certificate pinning methods, available in some browsers as well as in versions 3.5 and above of Microsoft’s Enhanced Mitigation Experience Toolkit (EMET).

4. Additional sources of information:

Apache: www.apache.org

NginX: http://nginx.org

Microsoft: http://support.microsoft.com

Apple: https://apple.com

OpenSSL: https://openssl.org

Opera: www.opera.com

Chrome: http://google.com/chrome

FireFox: http://mozilla.org

National Vulnerability Database: http://nvd.nist.gov

Disclaimer of Endorsement

The guidance in this document is provided "as is." In no event shall the United States Government be liable for any damages, regardless of the nature or theory of liability, arising in any way out of the use of or reliance on this guidance. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact Information

Industry Inquiries
410-854-6091
bao@nsa.gov
USG/IC Customer Inquiries
410-854-4790
DoD/Military/COCOM Customer Inquiries
410-854-4200
General Inquiries
NSA Information Assurance Service Center
niasc@nsa.gov

[i] "This POODLE Bites: Exploiting the SSL 3.0 Fallback - Security Advisory" Bodo Möller, Thai Duong, Krzysztof Kotowicz, September 2014

[ii] User interfaces and flags in FireFox vary based on the version, and obsolete flags are still shown in later versions. To be sure the settings are effective; restart the browser and retest.

[iii] Windows NT is no longer supported and is not considered secure. It is strongly recommended to update to a current, vendor-supported operating system.

[iv] FireFox 2 is no longer considered secure. Additional mitigations are required.

[v] Windows XP is no longer supported. Additional mitigations are required. It is strongly recommended to update to a current, vendor-supported operating system.

[vi] Earlier versions of iOS (listed) support TLS 1.2 but do not block SSL 3.0. The security update does not completely block SSL 3.0, but no CBC encryption modes are supported. Additional mitigations are required, especially if RC4 cipher suites are allowed.

[vii] Earlier versions of OSX support TLS 1.2 but do not block SSL 3.0. The security update does not completely block SSL 3.0, but no CBC encryption modes are supported. Additional mitigations are required, especially if RC4 cipher suites are allowed.